DETAILED ACTION

1. Applicant's amendment filed on June 2, 2008 has been entered. Claims 1-86 are pending. Claims 2, 5, 11, 41, 43, 46, 48, 56, 61, 63, 68, 71, 73, 76, 78, and 86 are cancelled by the applicant.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given by applicant on July 23, 2008. The applicant has agreed and authorized examiner to incorporate claims 5 and 11 into claim 1, claims 46 and 48 into claim 42, claims 61 and 63 into claim 57, claims 76 and 78 into claim 72 and to cancel claims 5, 11, 46, 48, 61, 63, 76, and 78.

CLAIMS:

3. Please cancel claims 5, 11, 46, 48, 61, 63, 76, and 78.

4. Please replace claims 1, 6, 12-16, 42, 47, 49, 57, 62, 64, 72, 77, and 79 as follows:

Claim 1. A computer-implemented method comprising: determining whether a source address for a first packet sent by the source address to a destination address qualifies as a threat, and when the source address qualifies as the threat, determining whether the destination address is synthetic; examining the first packet; determining a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat; when the destination address is determined to be not synthetic and the source address is the threat, determining whether the source address is on a local network; when the source address is determined to be on a local network and the source address qualifies as the threat, determining that the response comprises creating a synthetic hardware address, and performing for each respective device of a plurality of devices on the local network:

selecting the respective device, creating an address control protocol message comprising the synthetic hardware address as a message source address, inserting a corresponding hardware address for the respective device in the address control protocol message as a message destination hardware address, and sending the address control protocol message.

Claim 12. The method of claim 1 further comprising: performing the response.

Claim 13. The method of claim 1 wherein the creating the synthetic hardware address comprises ensuring that the synthetic hardware address is not in use on the local network.

Claim 14. The method of claim 1 further comprising: inserting a corresponding logical address for the respective device in the address control protocol message as a message destination logical address.

Claim 15. The method of claim 1 wherein the respective device inserts an entry into an address resolution protocol table in response to receiving the address resolution protocol message, wherein the entry comprises the synthetic hardware address as a source hardware address for the source address.

Claim 16. The method of claim 1 further comprising: when the source address is determined to be on the local network and the source address qualifies as the threat, determining that the response is to perform for each respective device of a plurality of devices on the local network: selecting the respective device, creating a respective synthetic hardware address for the respective device, creating an address control protocol message comprising the respective synthetic hardware address as a message source address, inserting a corresponding hardware address for a gateway communicating on behalf of the source address in the address control protocol message as a message destination hardware address, and sending the address control protocol message.

Claim 42. A system comprising: tangible computer readable medium with lo,qic instruction means executable by a computer processor including: threat-determining means for determining whether a source address for a first packet sent by the source address to a destination address qualifies as a threat; synthetic-address-determining means for determining whether the destination address is synthetic; examining means for examining the first packet; and response-determining means for determining a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat; location-determining means for determining whether the source address is on a local network; wherein when the location-determining means determine that the source address is on the local network and the source address qualifies as the threat, the response-determining means are configured to determine that the response is to create a synthetic hardware address, and perform for each respective device of a plurality of devices on the local network: select the respective device, create an address control protocol message comprising the synthetic hardware address as a message source address, insert a corresponding hardware address for the respective device in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Claim 47. The system of claim 42 wherein when the location-determining means determine that the source address is not on the local network and the source address qualifies as the threat, the response-determining means are configured to determine that the response is to perform for each respective device of a plurality of devices on the local network: select the respective device, create a respective synthetic hardware address for the respective device, create an address control protocol message comprising the respective synthetic hardware address as a message source address, insert a corresponding hardware address for a gateway communicating on behalf of the source address in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Claim 49. The system of claim 42 wherein when the location-determining means determine that the source address is on the local network and the source address qualifies as the threat, the response-determining means are configured to determine that the response is to perform for each respective device of a plurality of devices on the local network: select the respective device, create a respective synthetic hardware address for the respective device, create an address control protocol message comprising the respective synthetic hardware address as a message source address, insert the source address in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Claim 57. A system comprising: tangible computer readable medium with lo.qic instruction means executable by a computer processor including: a threat-determining module configured to determine whether a source address for a first packet sent by the source address to a destination address qualifies as a threat; a packet-type-determining module configured to determine a packet type of the first packet; an examining module configured to examine the first packet; and a response-determining module configured to determine a response to the first packet based upon the examining and based upon whether the source address qualifies as the threat; and a location-determining module configured to determine whether the source address is on a local network; wherein when the location-determining module determines that the source address is on the local network and the source address qualifies as the threat, the response-determining means are configured to determine that the response is to create a synthetic hardware address, and perform for each respective device of a plurality of devices on the local network: select the respective device, create an address control protocol message comprising the synthetic hardware address as a message source address, insert a corresponding hardware address for the respective device in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Claim 62. The system of claim 57 wherein when the location-determining module determines that the source address is not on the local network and the source address qualifies as the threat, the response-determining module is configured to determine that the response is to perform for each respective device of a plurality of devices on the local network: select the respective device, create a respective synthetic hardware address for the respective device, create an address control protocol message comprising the respective synthetic hardware address as a message source address, insert a corresponding hardware address for a gateway communicating on behalf of the source address in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Claim 64. The system of claim 57 wherein when the location-determining module determines that the source address is on the local network and the source address qualifies as the threat, the response-determining module is configured to determine that the response is to perform for each respective device of a plurality of devices on the local network: select the respective device, create a respective synthetic hardware address for the respective device, create an address control protocol message comprising the respective synthetic hardware address as a message source address, insert the source address in the address control protocol message as a message destination hardware address; and send the address control protocol message.

Claim 72. A computer product comprising: logic instruction embedded on computer-readable storage medium executable by a computer processor to cause the computer processor to: determine whether a source address for a first packet sent by the source address to a destination address qualifies as a threat; examine the first packet; determine whether the destination address is synthetic; determine a response to the first packet based upon the examining and whether the source address qualifies as the threat; and location-determining instructions configured to cause the computer processor to determine whether the source address is on a local network; wherein when

the location-determining instructions determines that the source address is on the local network and the source address qualifies as the threat, the instructions cause the computer processor to determine that the response is to create a synthetic hardware address, and perform for each respective device of a plurality of devices on the local network: select the respective device, create an address control protocol message comprising the synthetic hardware address as a message source address, insert a corresponding hardware address for the respective device in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Claim 77. The computer product of claim 72 wherein when the location-determining instructions determines that the source address is not on the local network and the source address qualifies as the threat, the instructions cause the computer processor to determine that the response is to perform for each respective device of a plurality of devices on the local network: select the respective device, create a respective synthetic hardware address for the respective device, create an address control protocol message comprising the respective synthetic hardware address as a message source address, insert a corresponding hardware address for a gateway communicating on behalf of the source address in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Claim 79. The computer product of claim 72 wherein when the location-determining instructions determines that the source address is on the local network and the source address qualifies as the threat, the instructions cause the computer processor to determine that the response is to perform for each respective device of a plurality of devices on the local network: select the respective device, create a respective synthetic hardware address for the respective device, create an address control protocol message comprising the respective synthetic hardware address as a message source address, insert the source address in the address control protocol message as a message destination hardware address, and send the address control protocol message.

Allowable Subject Matter

5. Claims 1, 3, 4, 6-10, 12-40, 42, 44, 45,47, 49-55, 57-60, 62, 64-67, 69, 70, 72, 74, 75, 77, and 79-85 are allowed. The following is an examiner's statement of reasons for allowance: Please see applicant's amendment filed June 2, 2008 and the telephone interview summary on July 23, 2008.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2135

TBT
July 27, 2008